Grid Security: Are We Making Progress?

A position paper for the DOE National Collaboratories Program Meeting

Marty Humphrey
University of Virginia, Charlottesville, VA, 22904, USA

As the Grid Forum turns five years old, it seems appropriate to assess the state of Grid security, particularly in the context of the contributions of the Grid Forum. This position paper contains two parts: the assessment of the state of the Grid Security community, and recommendations for future activities. This assessment is based on experience on the security architecture of Legion (1998-2001), user of Globus (2000 - present), director of OGSI.NET (2003 - present), director of WSRF.NET (2004 - present), and co-Director of the Security Area of the Grid Forum (1998 - present). The position paper is structured as a series of interrelated "Fact or Fiction" statements designed to be controversial and generate discussion.

How did we get here?

[1] *Security has always been emphasized in Grids.* Fact. The earliest days of Legion, Globus, and Unicore stressed the security issues related to sharing across administrative domains.

[2] *Grid Security papers don't get accepted at conferences because they lack graphs.* This is arguably Fiction. Rather, if they are written at all, Grid Security papers are often too difficult for the average reviewer to assess. In addition, these papers often contain "results" that are often unable to be reproduced.

[3] *Grid Security: Worst-case. Everything else: Average case or Once-in-a-blue-moon case.* Fact. The nature of security is to show that something *did not* happen or *will not* happen. The challenge is intrinsically more difficult than many of the other mechanisms necessary for national collaboratories.

[4] *We've been talking about "authorization interfaces" since GF1.* Fiction. We've *actually* only been talking about authorization interfaces since Grid Forum 2.

[5] *GSSAPI is overrated.* Fact. It's a complicated interface; there have been issues regarding "extending" it to support Grid requirements; it never really achieved the desired portability, as really there was ever only one implementation underneath it (GSI/PKI); and few people are ever actually exposed to this API (this will certainly be true for OGSI/WSRF).

[6] *Standards don't matter when there's only one implementation.* Fact. Any technology that only has to "interop" with itself does not face the scrutiny of independent implementations. In this is the case for any given technology, attempting to create "standards" is just wasted energy.

[7] *Passwords: good; PKI: bad.* This is Fact, certainly from the user perspective. And from the technical perspective, there are many factors that continue to inhibit the use of PKI in the wider community.

[8] *The Grid Community receives false comfort by making credentials "short-lived."* Fact. An attacker can do so many things in 8 hours.

[9] *There are few things new for security in Web Services -- people have been treading water as they SOAPify everything.* Fiction. While indeed the community *has* been treading water because of this, new approaches such as WS-Trust, WS-Policy, and WS-SecurityPolicy are capabilities that we have not seen in this community.

[10] *The emergence of businesses in GGF has not created the "fast pace of development necessary for business" but rather has bogged everything down.* Fiction. While the level of politics has increased substantially, there have been a number of incredibly bright new people participating in GGF.

[11] *Things have been going too well.* Fact. To date, there has not been one incident directly attributable to Grid security mechanisms or policies (noting that the recent "TeraGrid Incident" was *not* directly related to the Grid aspects). When this changes, our community will not be able to react accordingly.

How can we get where we need to go?

[1] *European projects (e.g., VOMS) are not disseminating enough.* Fact. The European projects are doing some really great work, but there is simply not an emphasis on getting other projects to use the software/protocols developed on a given project. This needs to change.

[2] *You thought OGSI was challenging -- wait until WSRF.* Fiction. Most of the core issues are similar. In fact, some are "easier" because WSRF is more consistent with pure Web Services. Hence, the community needs to continue addressing Web Services security, such as the services enumerated in the OGSA SEC architecture and roadmap documents.

[3] *Our community adequately leverages mainstream security and crypto research and results.* From one perspective, this is fiction, as the two communities seem to be isolated from each other. This may be because the Grid Security community is so closely tied to the application domains. On the other hand, this is fact -- our mission is to create a persistent, well-established security infrastructure, and the new techniques presented in mainstream computer security conferences are too unproven to be given to a widespread user base.

[4] *Risk models and threat models are properly utilized and discussed in the Grid security community.* Fiction. "Risk" and "threats" are rarely mentioned in this community. More emphasis must be placed on risk analysis, which would ultimately justify the research. More explicit treatment of attack models must be made across all existing and future Grid Security mechanisms.

[5] *The customer is always right.* Fact. In this case, the customer is the e-scientist. We must always keep in mind that our mission in the Grid security community is not to prevent access, but rather to enable controlled access. We must deliver the mechanisms that enable scientists to further their research. Better interfaces are particularly important.

[6] *We need to address the right problems: prevention, detection and limiting vulnerabilities, tolerance.* Fact. Particularly with regard to "tolerance", our community must acknowledge that attacks will successfully occur, and more attention must be made to handle and contain these attackers once they are inside the perimeter.

[7] *Policy is going to kill us.* Fact. "Policy" is generally viewed as "Security Policy", so the broader Grid community will be looking for the Grid Security community to "solve" policy issues. This is an extremely complex set of issues that are not easily solved. We need to begin to build ways in which to express, negotiate, and enforce policies.

Fact or Fiction: ***The Grid Security community is making progress.*** This is FACT, although much more can be done. With the introduction of WSRF, in particular, and its reliance on Web Services standards and tooling, there are almost an unbounded set of opportunities for the Grid security community to provide working solutions to critical security issues for national collaboratories.